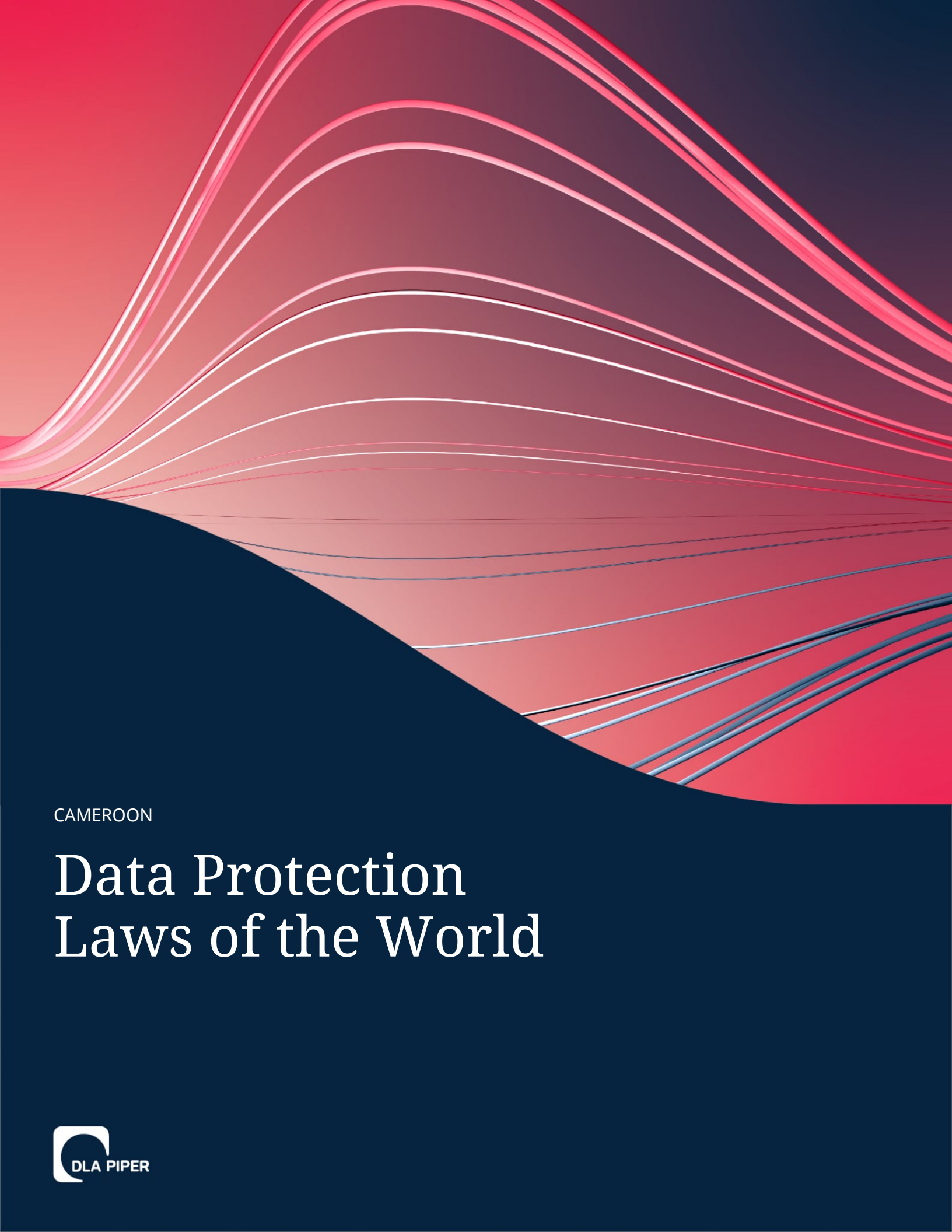




CAMEROON

Data Protection Laws of the World

Introduction



Welcome to the 15th update of the Data Protection Laws of the World handbook. Data protection and privacy laws continue to evolve at pace, reflecting responses to technological change, increasing data-driven business models and heightened expectations around accountability and enforcement. Alongside jurisdiction-specific reform, a number of clear global trends are emerging, including increasing enforcement action, greater data localization and complexities with data transfers, and closer alignment between data protection, cybersecurity and wider digital regulation, all set within a backdrop of heightened geopolitical tensions. As a result, keeping track of developments across jurisdictions has become both more important and more challenging for organisations operating internationally.

Recent legislative and enforcement developments

This edition reflects another busy year for privacy and data protection, with new legislation taking effect in key markets such as India, while enforcement of established data protection laws, such as those in Europe, continues to be influenced by an increasingly complex geopolitical environment and escalating cyber threats.

Developments in the United States

In the United States, consumer privacy laws continue to rapidly develop at the state level, with the passage of more than 20 state comprehensive consumer privacy laws and increased state and multi-state enforcement. Recently, minor privacy laws have been passed and taken effect in a number of states, imposing privacy obligations and restrictions on websites and online services that provide services that are directed at minors under 18 years old or that collect personal information about known minors under 18 years old. In addition to increased regulator enforcement, privacy litigation is on the rise in the United States – key areas of focus for privacy litigation and class action risk include minor privacy and safety, online tracking, data breaches and cyber incidents, text marketing, and biometrics.

Responding to a rapidly evolving landscape

To support clients in navigating this fast-moving landscape, Data Protection Laws of the World will now be updated twice per year, reflecting the accelerating pace of reform within the data protection and privacy landscape and the growing need for up-to-date, practical insight.



Data protection laws

The data protection regime in Cameroon is governed by the following laws and regulations:

- Law No. 2024/017 of 23 December 2024 on the protection of personal data
- Law N°2010/013 of 21 December 2010 governing electronic communications in Cameroon
- Law No. 2010/012 of 21 December 2010 on cybersecurity and cybercrime in Cameroon
- Law N°2016/007 of 12 July 2016 on the Criminal Code
- Law No 2010/021 of 21 December 2010 on electronic commerce in Cameroon
- Framework Law N° 2011/012 of 06 May 2011 on Consumer Protection in Cameroon
- Decree N° 2011/1521/PM of 11 June 2011 laying down the implementing provisions of Law No 2010/021 of 21 December 2010 on electronic commerce in Cameroon
- Decree No. 2019/150 of 22 March 2019 on the Organisation and Functioning of the National Information and Communication Technology Agency (ANTIC)
- Regulation No. 03/16-CEMAC-UMAC-CMAC-CM of 21 December 2016 on Systems, Means and Incidents of Payment
- Law No. 2023/009 of 25 July 2023 on the Charter for the Protection of Children Online in Cameroon
- Project Draft Decree No. laying down the implementing provisions of the Data Protection Act in Cameroon

Definitions

Definition of personal data

Information relating to a person enabling that person to be identified directly or indirectly, in particular by reference to any form of identifier or to one or more

elements specific to their physical, psychological, genetic, psychological, cultural, socio-professional or economic identity, in particular a name, a photograph, a fingerprint, a postal address, an e-mail address, a telephone number, a social security number, an internal personnel number, a digital identifier, an IP address, a computer connection identifier or a voice recording. (Article 5 of the Data Protection Act)

Definition of sensitive personal data

Information relating in particular to religious, philosophical, political or trade union opinions and activities, banking transactions, racial or ethnic origin, linguistic or regional origin, sex life, genetics, biometrics, health, legal proceedings and criminal sanctions (Article 5 of the Law).

National data protection authority

Cameroon's Data Protection Authority is an independent public body responsible for, among other things:

- ensuring the application of this law, the texts adopted for its application and international conventions on the subject;
- issuing the authorisations provided for in this law, together with the relevant specifications;
- drawing up, publishing and updating the reference system of technical and organisational measures for personal data;
- approve the certification mechanisms for personal data processing processes and techniques;
- dealing with complaints, petitions and claims lodged by a data subject or by a body, organisation or association and, to the extent necessary, examining or investigating the subject of said complaints, petitions or claims, and informing the author of the complaint, petition or claim of the progress and outcome of the investigation within a reasonable period of time;
- draw up and publish a list of countries recognised as offering a level of protection of personal data equivalent to the requirements under Cameroonian law;
- to cooperate with other authorities responsible for the protection of personal data, in liaison with the administrations and structures concerned.

Registration

Article 19 of the 2024 Law provides that the processing of personal data is subject to prior authorisation issued by the Personal Data Protection Authority. Article 27 of the Draft Decree provides for 3 types of authorisations:

- prior notice,
- prior declaration and
- prior authorisation.

Further, Article 39 (1) provides that the controller or processor shall keep a physical or digital register of the processing operations carried out under his/her responsibility.

The register shall contain the following information:

- the name and contact details of the controller and, where applicable the name of the processor
- the purposes of processing data
- a description of the categories of data subjects and personal data
- the categories of recipients to whom the personal data have been or will be disclosed
- documents attesting to the existence of appropriate safeguards or the number of the authorization issued by the Personal Data Protection Authority

Data protection officers

Article 38 of the Draft of 2024 Data Protection Law provided for the mandatory appointment of a DPO not on the basis of the size of the company but rather on the type and quantity of data processed, the systematic nature of the processing or the number of persons concerned by the processing carried out by the company. However, the final version of the law adopted did not include this provision. It is, therefore, likely that this point will be regulated in the Decree implementing the 2024 law on data protection or a subsequent regulatory text of the Ministry of Posts and Telecommunications.

Collection and processing

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data.

These include:

- **consent and legitimacy:** unless otherwise provided by law, data controllers are obligated to obtain consent from the data subject
- **purpose:** personal data can only be collected and processed for a specific and legitimate purpose
- **proportionality and relevance:** personal data must only be processed in a relevant and necessary manner regarding the purpose and objectives of the processing
- **lawfulness and fairness:** data controllers must collect and process data in a fair, lawful, and not fraudulent manner
- **data retention:** a specified period of time should be determined in advance depending on the purpose of processing to ensure that personal data is not stored indefinitely
- **security and confidentiality:** all responsible persons for processing personal data must not only ensure the security of data or files to prevent their destruction, or

alteration; but also prevent unauthorized access to personal data contained in a file or intended to form part of the files

- **prior formalities:** the processing of personal data and any interconnection and interoperability of sensitive data files relating to minors is subject to prior authorisation from the data protection authority.

Transfer of personal data

The transfer of personal data to a foreign country or to an international organisation is subject to prior authorisation being obtained from the Personal Data Protection Authority under conditions that guarantee the exercise of the data subject's rights.

When issuing such authorisation, the Personal Data Protection Authority must first ensure that:

- that the country of destination of the personal data offers an adequate level of protection;
- the prior entry into force of a legal instrument signed with the country of destination of the personal data transferred, in liaison with the competent authorities and bodies;
- the entity requesting the import of personal data is subject to binding security rules for the protection of such data
- the prior subscription, by the importing and exporting entities concerned, of standard contractual clauses relating to the international transfer of personal data, drawn up and published by the Personal Data Protection Authority.

Security

A reference framework for security, technical and organizational measures will be established by the Personal Data Protection Authority.

Breach notification

Once the controller or processor are aware of a personal data breach, he/she must immediately inform the Personal Data Protection Authority and the data subject. The draft of the bill provided for a 72-hour timeline.

Enforcement

The Law No. 2024/017 of 23 December 2024 on the protection of personal data is too recent.

The Decree implementing the provisions of the law is not yet adopted.

Other Ministerial Order are still awaited.

Consequently, we have not identified any significant application decisions for the time being.

Electronic marketing

Articles 32 of Law No 2010/021 of 21 December 2010 on electronic commerce in Cameroon of states that all service providers are required to store and preserve the data relating to any commercial transaction made electronically in accordance with applicable laws and regulations.

Further, direct prospecting by means of an automated calling machine, a fax machine or an electronic mail using, in any form whatsoever, the contact details of a natural or legal person who has not expressed his prior consent to receive direct prospecting by this means is prohibited (art. 7 (1)).

Online privacy

The law does not lay down specific rules for cookies and location data.

As the law on data protection is very recent, it is likely that cookies and location data will be provided for in the reference framework that will be established by the Personal Data Protection Authority or be the subject of a regulatory text of the Ministry of Posts and Telecommunications in the coming days.

Data protection lawyers



Basile Mayoue
Of Counsel
Geni & Kebe
b.mayoue@gsklaw.sn



Tano Andi Germain
Counsel
Geni & Kebe
a.tano@gsklaw.sn

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
carolyn.bigg@dlapiper.com
[Full bio](#)



John Magee

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
john.magee@dlapiper.com
[Full bio](#)



Andrew Serwin

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
andrew.serwin@us.dlapiper.com
[Full bio](#)

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com